ABSTRACT

~~Improvements Relating To Document Transmission Techniques~~

A method of determining the authenticity of a digital document sent by an unknown sender. The method comprises receiving a digital document and an encrypted digest of the document created by the sender using a hash algorithm. The digest is encrypted using a first token, such as a private key, of the sender. The method also comprises obtaining a second token, such as a public key, relating to the first token, decoding the encrypted digest using the second token, using a hash algorithm to create a digest of the document; and comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document. The receiving step may comprise receiving a digital certificate of the sender within which the second token is contained as part of the sender's digital certificate. Also the validity of the sender's certificate can be checked on-line.

~~(Figure 4)~~